Technical Defense, Inc
strategic information outcomes

TERRORISM
RESEARCH CENTER

Cyberterrorism

Identifying and Responding to New Threats

June 18, 2002

Matthew G. Devost

Terrorism Research Center, Inc. & Technical Defense, Inc.

About Me – Matthew G. Devost

- Researching Implications of Information Technology on National Security since 1993.
- Creator and Director of the first Coalition Vulnerability Assessment Team (U.S., NATO, Canada, U.K., Australia, New Zealand)
- Founding Director of the Terrorism Research Center, Inc.
- Award winning author on information terrorism issues
- Directly involved in many assessments around the world (commercial and gov't)
- Support to international corporations and governments including FBI, Joint Staff, Microsoft, Citigroup, Swedish Government, PCCIP, NSTAC, Defense Science Board, DISA, OMNCS, FAA, etc.

TERRORISM RESEARCH CENTER

U.S. CUSTOMS SERVICE 1789

SAIC An Employee-Owned Company

iDEFENSE

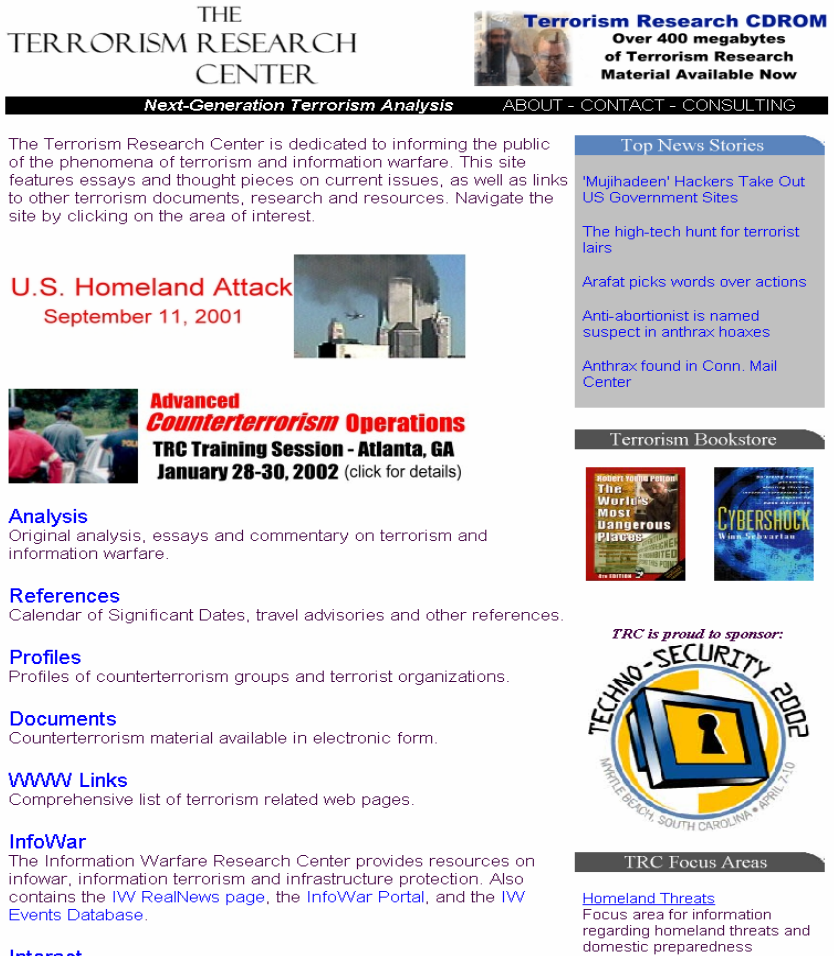
Security Design INTERNATIONAL

Counterpane Internet Security

Technical Defense, Inc strategic information outcomes

Public Web site

TERRORISM RESEARCH CENTER



THE TERRORISM RESEARCH CENTER

Terrorism Research CDROM
Over 400 megabytes
of Terrorism Research
Material Available Now

Next-Generation Terrorism Analysis ABOUT - CONTACT - CONSULTING

The Terrorism Research Center is dedicated to informing the public of the phenomena of terrorism and information warfare. This site features essays and thought pieces on current issues, as well as links to other terrorism documents, research and resources. Navigate the site by clicking on the area of interest.

U.S. Homeland Attack
September 11, 2001

Advanced *Counterterrorism* Operations
TRC Training Session - Atlanta, GA
January 28-30, 2002 (click for details)

Analysis
Original analysis, essays and commentary on terrorism and information warfare.

References
Calendar of Significant Dates, travel advisories and other references.

Profiles
Profiles of counterterrorism groups and terrorist organizations.

Documents
Counterterrorism material available in electronic form.

WWW Links
Comprehensive list of terrorism related web pages.

InfoWar
The Information Warfare Research Center provides resources on infowar, information terrorism and infrastructure protection. Also contains the IW RealNews page, the InfoWar Portal, and the IW Events Database.

Top News Stories

'Mujihadeen' Hackers Take Out US Government Sites

The high-tech hunt for terrorist lairs

Arafat picks words over actions

Anti-abortionist is named suspect in anthrax hoaxes

Anthrax found in Conn. Mail Center

Terrorism Bookstore

TRC is proud to sponsor:

TRC Focus Areas

Homeland Threats
Focus area for information regarding homeland threats and domestic preparedness

WWW.TERRORISM.COM

5,000,000+ hits/month

5000+ links into site

Numerous awards

Original content

TRC Recent and Current Initiatives

Massachusetts Bay Transportation Authority

MIPT Oklahoma City National Memorial Institute for the Prevention of Terrorism

Preventing and deterring terrorism or mitigating its effects

CENTRAL ARTERY TUNNEL

FEDERAL AVIATION ADMINISTRATION

BART

JOINT CHIEFS OF STAFF

ATA AMERICAN TRUCKING ASSOCIATIONS

massport

National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

Quotes

The most likely perpetrators of cyber attacks on critical infrastructures are terrorists and criminal groups rather than nation-states.

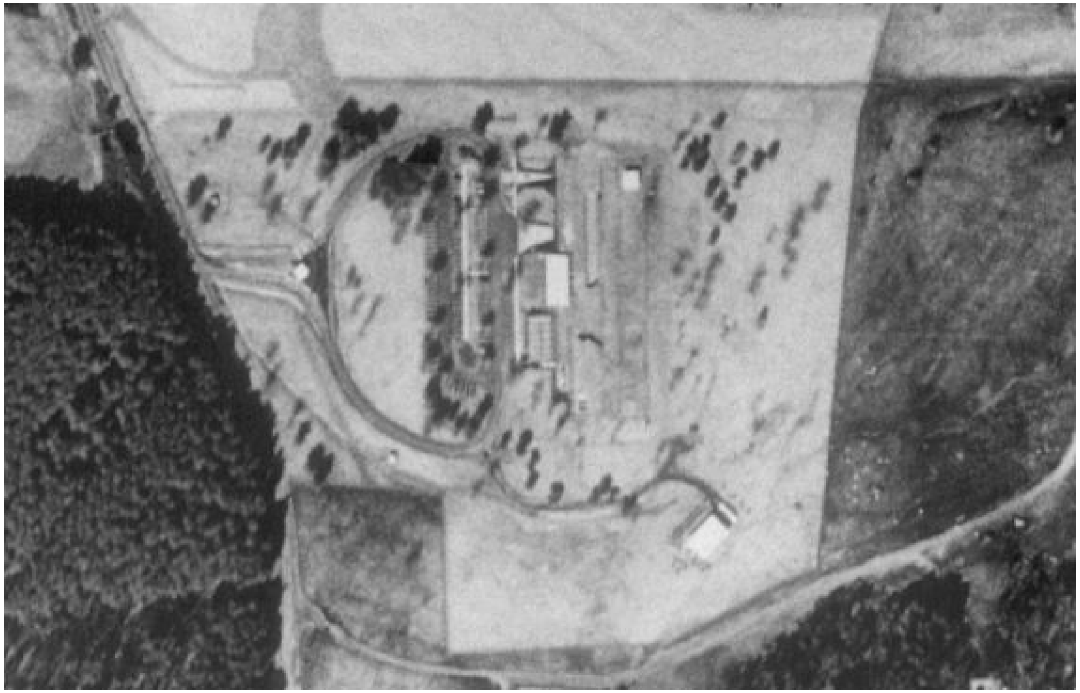
– The Gilmore Commission

Not "Crude and Unsophisticated"

Cyber terrorism is extremely difficult to guard against. Cyber terrorists are often well educated, with the expertise and equipment to stay ahead of advances in protective security. Yet, the havoc wreaked by a major cyber-attack could be enormous.

– 1999 Report of the Special Senate Committee on Security and Intelligence (CANADA)

Information Terrorism Overview



Is this a hard target or a soft target?
Picture of Mount Pony Bunker, Culpeper, VA

Critical Infrastructure Threat Matrix

Infrastructure Threat Matrix		**Target**	
		Physical	*Digital*
Tool	*Physical*	(a) Conventional Terrorism (Oklahoma City Bombing)	(b) IRA attack on London Square Mile, 4 Oct 1992
	Digital	(c) Spoof Air Traffic Control to crash plane.	(d) "Pure" Information Terrorism (Trojan horse in public switched network)

Cell (d) the most difficult to detect and counter

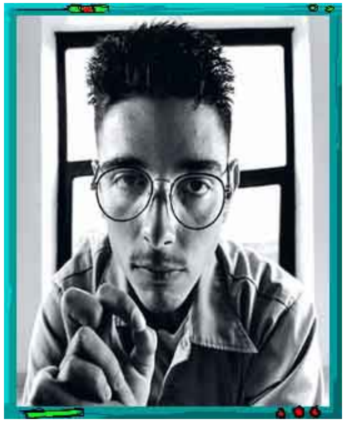
Information Terrorism
Recent Threat Activity

“Hacktivists” Of All Persuasions Take Their Struggle To The Web

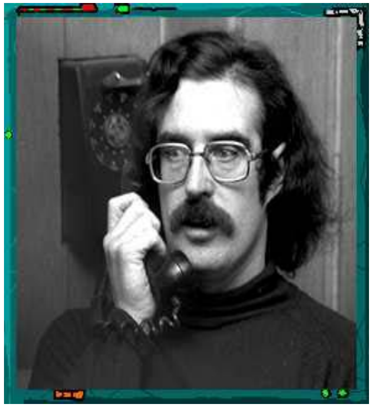
Threat Trends - Agents

- Automated tools allow for unsophisticated hackers to launch devastating attacks (e.g. Mafiaboy)
- Increasing focus on CNA within terrorist organizations (prior to 9/11/01)
  - Younger, technical membership
  - Sponsoring graduate degrees in computer science
- As physical security measures are enhanced (post 9/11/01) and resources are restricted, electronic attack becomes even attractive, especially against critical infrastructure targets

Past Threat Profile (Time for a new one?)



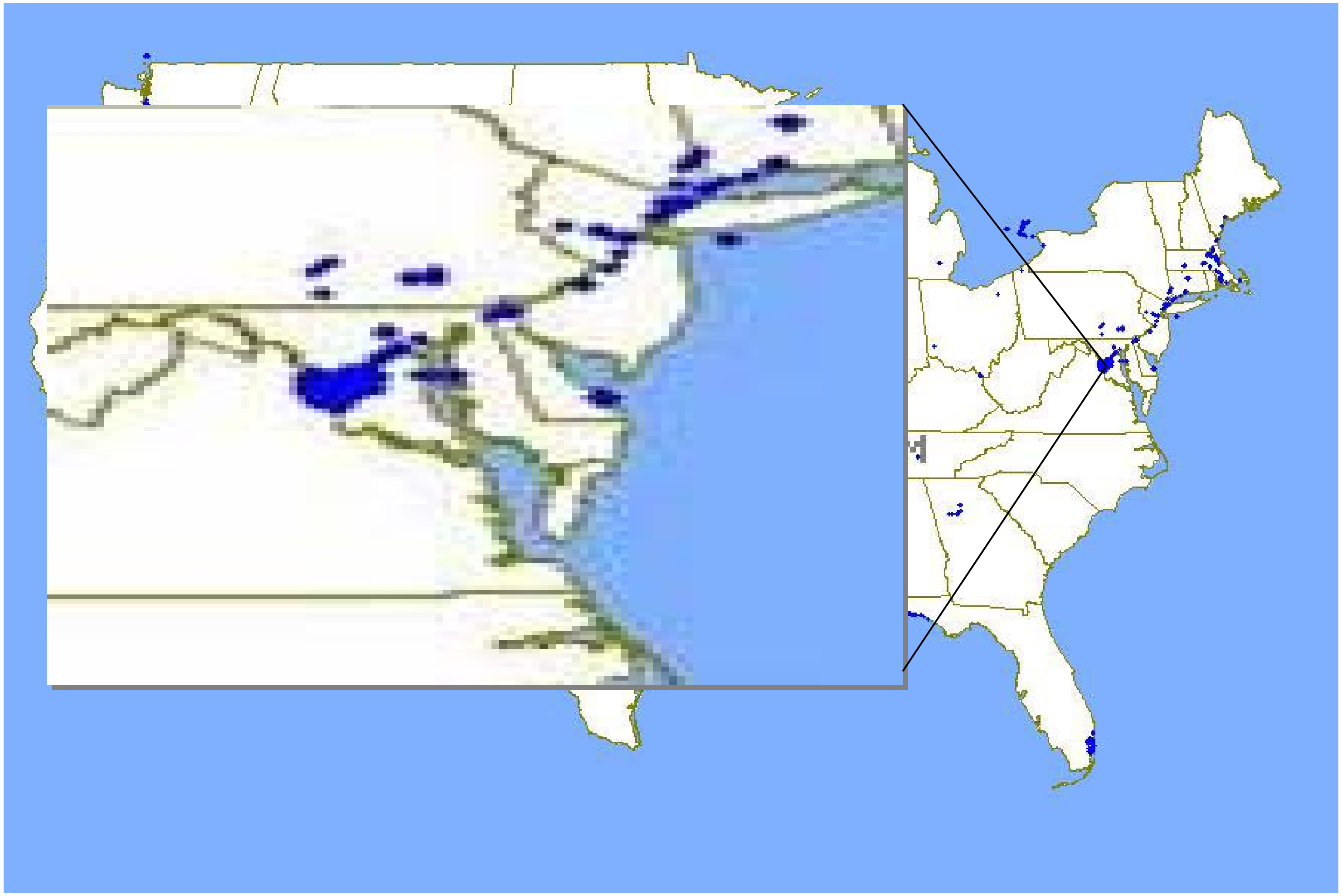
"the most organized and systematic attack the Pentagon has seen to date"



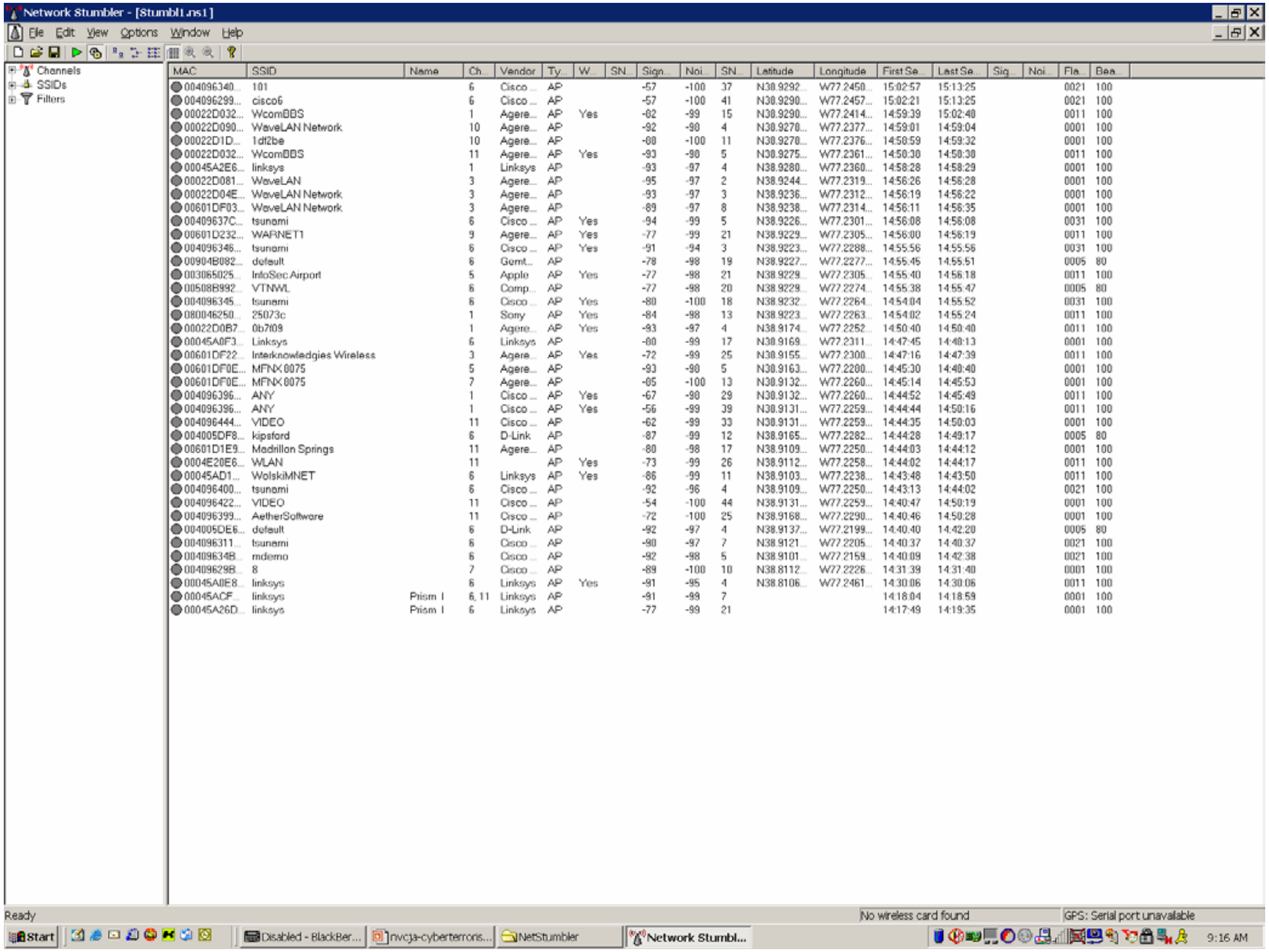
Threat Trends - Tools

- Attack tools are increasingly automated and stealthy
- Distributed Denial of Service
- Rapidly propagating worms
- Multi-functional and cross platform attack tools
- Exploit emerging technologies (e.g. wireless)
- Incredibly dynamic capabilities emerging
  - “Goner” attacking via email and instant messaging

Attacking Wireless Networks



Wireless Networks – Route 7, NOVA



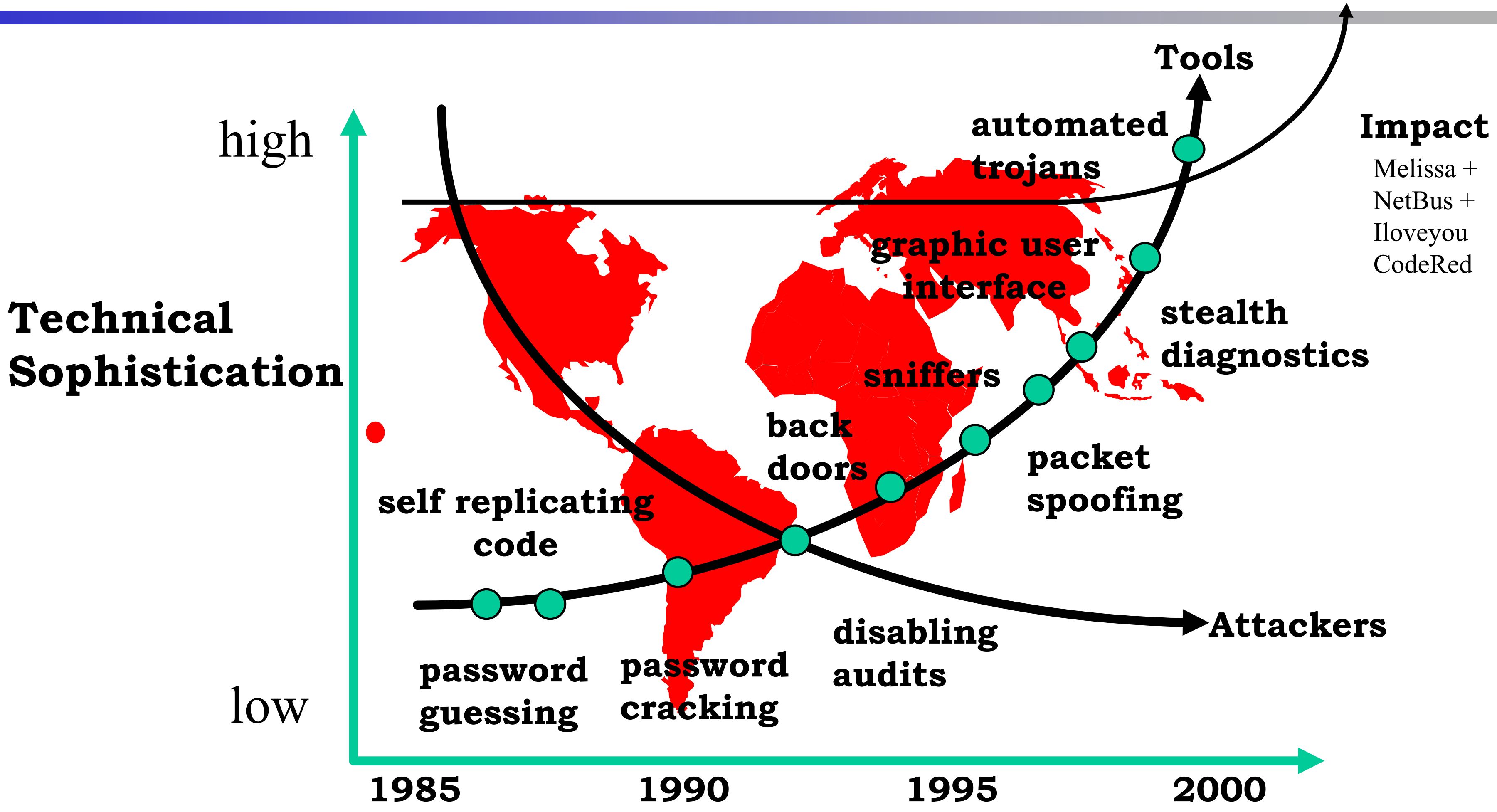
MAC	SSID	Name	Ch...	Vendor	Ty...	W...	SN...	Sign...	Noi...	SN...	Latitude	Longitude	First Se...	Last Se...	Sig...	Noi...	Fla...	Bea...
● 004096340...	101		6	Cisco ...	AP			-57	-100	37	N30.9292...	W77.2450...	15:02:57	15:13:25			0021	100
● 004096299...	cisco6		6	Cisco ...	AP			-57	-100	41	N30.9290...	W77.2457...	15:02:21	15:13:25			0021	100
● 00022D032...	WcomBBS		1	Agere...	AP	Yes		-02	-99	15	N30.9290...	W77.2414...	14:59:39	15:02:40			0011	100
● 00022D090...	WaveLAN Network		10	Agere...	AP			-92	-90	4	N30.9270...	W77.2377...	14:59:01	14:59:04			0001	100
● 00022D1D...	1df2be		10	Agere...	AP			-00	-100	11	N30.9270...	W77.2376...	14:50:59	14:59:32			0001	100
● 00022D032...	WcomBBS		11	Agere...	AP	Yes		-93	-90	5	N30.9275...	W77.2361...	14:50:30	14:50:30			0011	100
● 00045A2E6...	linksys		1	Linksys	AP			-93	-97	4	N38.9280...	W77.2360...	14:58:28	14:58:29			0001	100
● 00022D081...	WaveLAN		3	Agere...	AP			-95	-97	2	N38.9244...	W77.2319...	14:56:26	14:56:28			0001	100
● 00022D04E...	WaveLAN Network		3	Agere...	AP			-93	-97	3	N38.9236...	W77.2312...	14:56:19	14:56:22			0001	100
● 00601DF03...	WaveLAN Network		3	Agere...	AP			-89	-97	8	N38.9238...	W77.2314...	14:56:11	14:56:35			0001	100
● 00409637C...	tsunami		6	Cisco ...	AP	Yes		-94	-99	5	N38.9226...	W77.2301...	14:56:08	14:56:08			0031	100
● 00601D232...	WARNET1		9	Agere...	AP	Yes		-77	-99	21	N38.9229...	W77.2305...	14:56:00	14:56:19			0011	100
● 004096346...	tsunami		6	Cisco ...	AP	Yes		-91	-94	3	N38.9223...	W77.2288...	14:55:56	14:55:56			0031	100
● 00904B082...	default		6	Gemt...	AP			-78	-98	19	N38.9227...	W77.2277...	14:55:45	14:55:51			0005	80
● 003065025...	InfoSec Airport		5	Apple	AP	Yes		-77	-98	21	N38.9229...	W77.2305...	14:55:40	14:56:18			0011	100
● 00508B992...	VTNWL		6	Comp...	AP			-77	-98	20	N38.9229...	W77.2274...	14:55:38	14:55:47			0005	80
● 004096345...	tsunami		6	Cisco ...	AP	Yes		-80	-100	18	N38.9232...	W77.2264...	14:54:04	14:55:52			0031	100
● 080046250...	25073c		1	Sony	AP	Yes		-84	-98	13	N38.9223...	W77.2263...	14:54:02	14:55:24			0011	100
● 00022D0B7...	0b7f09		1	Agere...	AP	Yes		-93	-97	4	N38.9174...	W77.2252...	14:50:40	14:50:40			0011	100
● 00045A0F3...	Linksys		6	Linksys	AP			-00	-99	17	N30.9169...	W77.2311...	14:47:45	14:40:13			0001	100
● 00601DF22...	Interknowledgies Wireless		3	Agere...	AP	Yes		-72	-99	25	N30.9155...	W77.2300...	14:47:16	14:47:39			0011	100
● 00601DF0E...	MFNX 0075		5	Agere...	AP			-93	-90	5	N30.9163...	W77.2280...	14:45:30	14:40:40			0001	100
● 00601DF0E...	MFNX 0075		7	Agere...	AP			-05	-100	13	N30.9132...	W77.2260...	14:45:14	14:45:53			0001	100
● 004096396...	ANY		1	Cisco ...	AP	Yes		-67	-90	29	N30.9132...	W77.2260...	14:44:52	14:45:49			0011	100
● 004096396...	ANY		1	Cisco ...	AP	Yes		-56	-99	39	N30.9131...	W77.2259...	14:44:44	14:50:16			0011	100
● 004096444...	VIDEO		11	Cisco ...	AP			-62	-99	33	N30.9131...	W77.2259...	14:44:35	14:50:03			0001	100
● 004005DF8...	kipsford		6	D-Link	AP			-87	-99	12	N38.9165...	W77.2282...	14:44:28	14:49:17			0005	80
● 00601D1E9...	Madrillon Springs		11	Agere...	AP			-80	-98	17	N38.9109...	W77.2250...	14:44:03	14:44:12			0001	100
● 0004E20E6...	WLAN		11		AP	Yes		-73	-99	26	N38.9112...	W77.2258...	14:44:02	14:44:17			0011	100
● 00045AD1...	WolskiMNET		6	Linksys	AP	Yes		-86	-99	11	N38.9103...	W77.2238...	14:43:48	14:43:50			0011	100
● 004096400...	tsunami		6	Cisco ...	AP			-92	-96	4	N38.9109...	W77.2250...	14:43:13	14:44:02			0021	100
● 004096422...	VIDEO		11	Cisco ...	AP			-54	-100	44	N38.9131...	W77.2259...	14:40:47	14:50:19			0001	100
● 004096399...	AetherSoftware		11	Cisco ...	AP			-72	-100	25	N38.9168...	W77.2290...	14:40:46	14:50:28			0001	100
● 004005DE6...	default		6	D-Link	AP			-92	-97	4	N38.9137...	W77.2199...	14:40:40	14:42:20			0005	80
● 004096311...	tsunami		6	Cisco ...	AP			-90	-97	7	N38.9121...	W77.2205...	14:40:37	14:40:37			0021	100
● 00409634B...	mdemo		6	Cisco ...	AP			-92	-98	5	N38.9101...	W77.2159...	14:40:09	14:42:38			0021	100
● 00409629B...	8		7	Cisco ...	AP			-89	-100	10	N38.8112...	W77.2226...	14:31:39	14:31:40			0001	100
● 00045A0E8...	linksys		6	Linksys	AP	Yes		-91	-95	4	N38.8106...	W77.2461...	14:30:06	14:30:06			0011	100
● 00045ACF...	linksys	Prism I	6, 11	Linksys	AP			-91	-99	7			14:18:04	14:18:59			0001	100
● 00045A26D...	linksys	Prism I	6	Linksys	AP			-77	-99	21			14:17:49	14:19:35			0001	100

Ready

No wireless card found

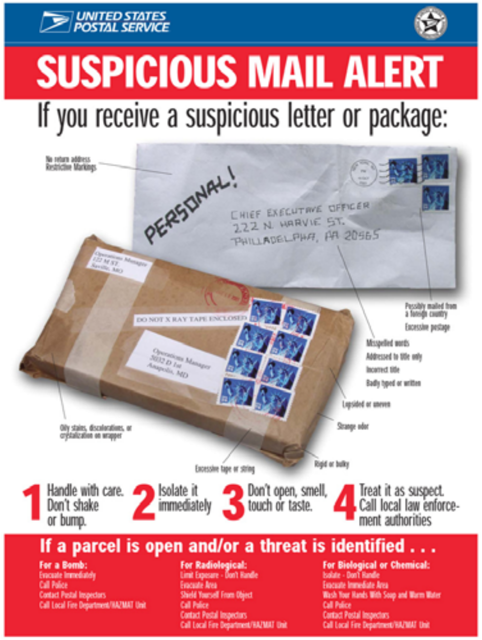
GPS: Serial port unavailable

Evolution of Hacker Tools



Threat Trends - Targets

Kill with a borrowed sword…



UNITED STATES POSTAL SERVICE

SUSPICIOUS MAIL ALERT

If you receive a suspicious letter or package:

No return address
Restrictive Markings
PERSONAL!
CHIEF EXECUTIVE OFFICER
222 N. HARVIE ST.
PHILLADELPHIA, PA 20565
Operations Manager
122 M ST.
Saville, MO
DO NOT X RAY TAPE ENCLOSED
Operations Manager
3032 D 1st
Anapolis, MD
Possibly mailed from a foreign country
Excessive postage
Misspelled words
Addressed to title only
Incorrect title
Badly typed or written
Lopsided or uneven
Strange odor
Rigid or bulky
Excessive tape or string
Oily stains, discolorations, or crystalization on wrapper

1 Handle with care. Don't shake or bump.

2 Isolate it immediately

3 Don't open, smell, touch or taste.

4 Treat it as suspect. Call local law enforcement authorities

If a parcel is open and/or a threat is identified . . .

For a Bomb:
Evacuate Immediately
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

For Radiological:
Limit Exposure - Don't Handle
Evacuate Area
Shield Yourself From Object
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

For Biological or Chemical:
Isolate - Don't Handle
Evacuate Immediate Area
Wash Your Hands With Soap and Warm Water
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

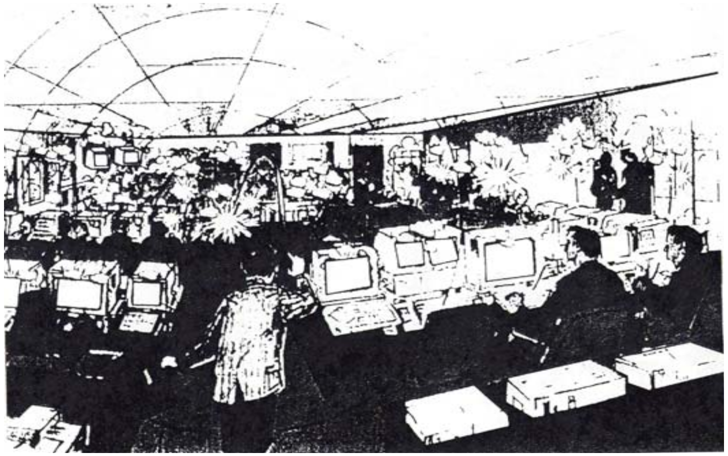
Threat Techniques

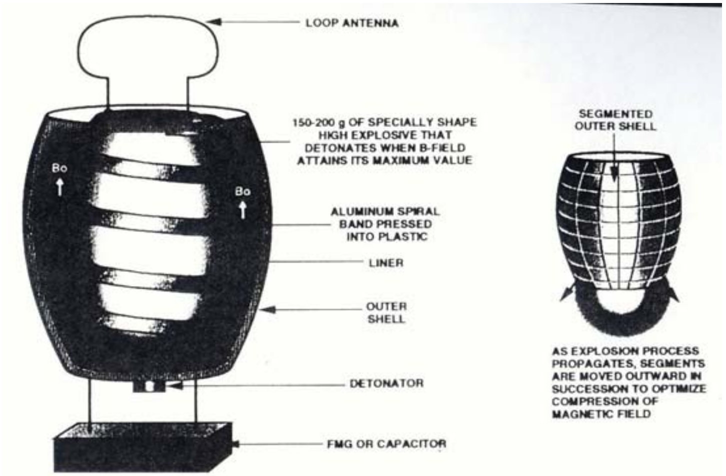
Masquerading
Electronic Warfare
Intrusion/Hacking
Directed Energy
PSYOP
Diversion
Insider Placement
Distributed Denial of Service

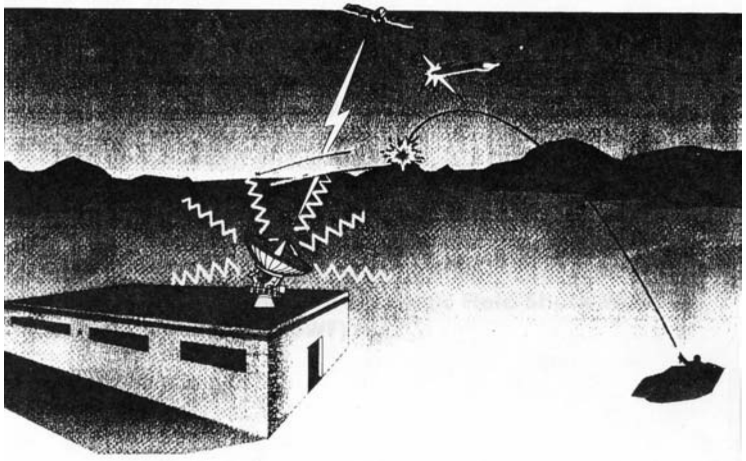
Spoofing
Signals Intel
Substitution/Mod.
Deception
Misinformation
Denial of Service
Malicious Code

Blue = Most attractive to terrorist organizations.

HERF Threats?




LOOP ANTENNA
150-200 g OF SPECIALLY SHAPE HIGH EXPLOSIVE THAT DETONATES WHEN B-FIELD ATTAINS ITS MAXIMUM VALUE
Bo
Bo
ALUMINUM SPIRAL BAND PRESSED INTO PLASTIC
LINER
OUTER SHELL
DETONATOR
FMG OR CAPACITOR
SEGMENTED OUTER SHELL
AS EXPLOSION PROCESS PROPAGATES, SEGMENTS ARE MOVED OUTWARD IN SUCCESSION TO OPTIMIZE COMPRESSION OF MAGNETIC FIELD



Traditional Threat Goals

- Unauthorized Disclosure of Data
  - Access to secrets!
- Corruption of Data
  - Can no longer trust the data we have
- Denial of Service
  - You will not communicate or perform other needed functions.
- Disruption of Communications
  - Make it harder to communicate
  - Communications become unreliable

Threat Goals - The Future

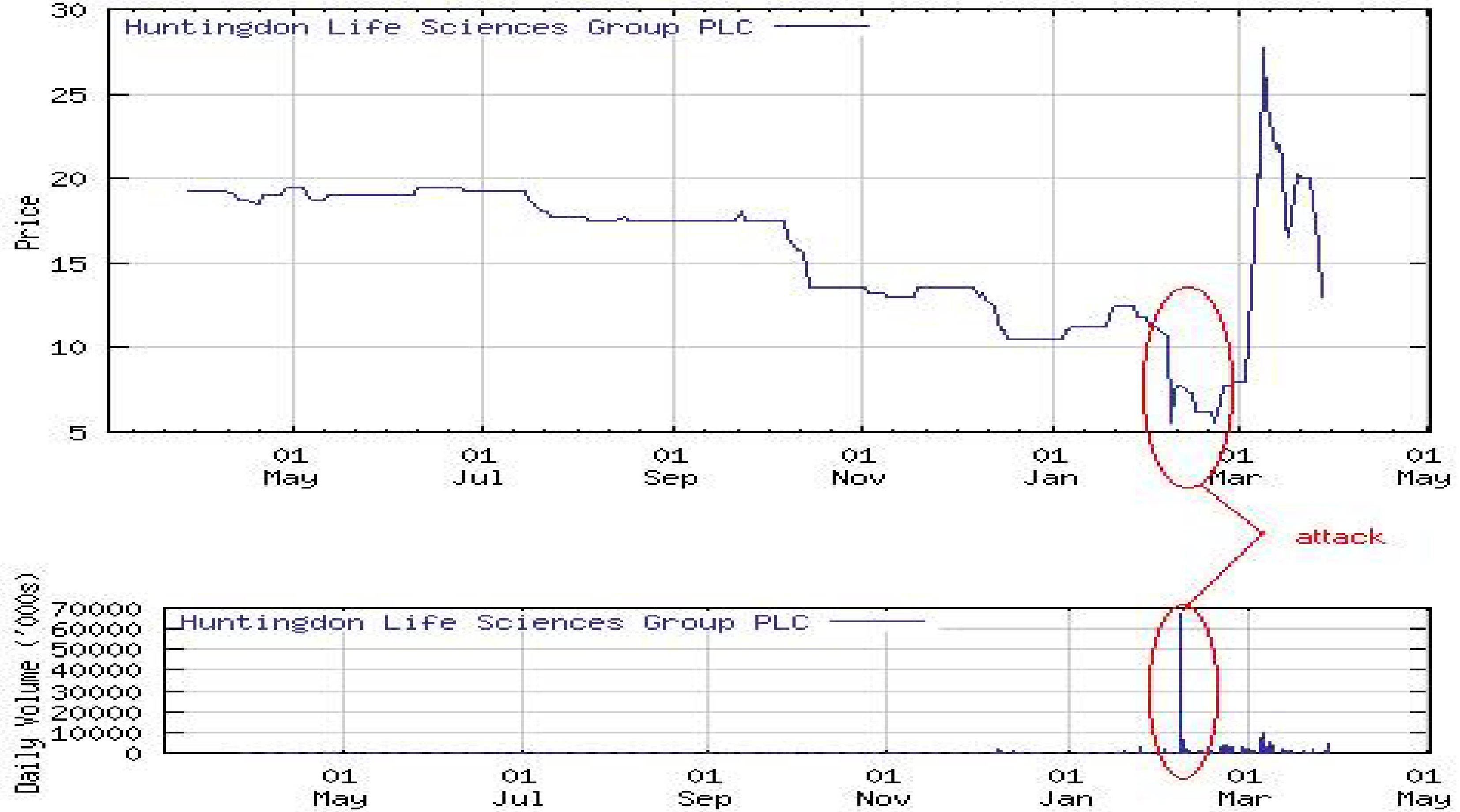
- Disruption of Social Integrity
  - Target Critical Infrastructures (Decrease Confidence)
  - Create public panic and distrust
  - Disrupt financial systems
  - Kill power to major city during play-off celebration
- Deter Force Projection
  - The Somalia Scenario, infrastructure attacks, PSYOP
- Fund Threat Activities
  - IW in support of making money.
  - Influence markets, etc.
    - E.g. - Advance knowledge of press releases, labor statistics.

Influencing Markets Seem Far Fetched?

NEW YORK (AP) -- A Houston man was arrested Thursday on charges that he violated securities laws by posting a phony press release on the Internet that caused the stock of Lucent Technologies to plunge in value.

Manhattan prosecutors accused Fred Moldofsky, 43, of causing the value of the stock in the world's top manufacturer of communications equipment to fall as much as 3.6 percent, from $62.62 to $60.37. **That trimmed the value of the company on Wall Street by $7.1 billion.**

The Power of Influence?



Source: Wanja Eric Naef, www.iwar.org.uk

The Known Threats

- Criminal Hackers
  - Credit card/bank fraud, information theft, and personal attacks
  - Malicious intent!
- Curious Hackers
  - New exploits, conferences, and white papers
  - Have merged into community as security experts - advising the government
    - L0pht/@Stake/White House, DefCon conferences, etc

The Known Threats (II)

- Corporate Espionage
  - Hacking for competitive advantage
    - See Winkler - “Corporate Espionage”
    - See Fialka - “War by Other Means”
  - What’s next? Creating competitive advantage?

The Known Threats

- 100+ Nations developing capabilities **(5/18/2000)**
- Russia - Scared of the IW threat
  - Yelstin "While maintaining our nuclear potential at the proper level, we need to devote more attention to developing the entire range of means of information warfare."
- China - IW is the next people's war
  - "Unrestricted Warfare" book released
  - Significant implications!
- Israel - Analyzer "Damn Good!"

The Emerging Threats

- Terrorist Organizations
  - Using the web as information tool
  - Collect targeting information (reduces casing exposure)
  - Coordinate activities (e.g. shoe bomber email)
  - Soliciting hackers?
  - Electronic attacks against counterterrorism firms
- Hacktivists
  - Winn Schwartau, “If we had your skills (hackers) in the 60s, the 80s would have never happened!”
  - Memphis Example, Electronic Disturbance Theatre
  - **Earth Liberation Front** announces inclusion of electronic attacks in arsenal

Hactivists and Activists

- Combining electronic and physical protest tactics
- Increasingly sophisticated support infrastructure for protests against international organizations/meetings
  - Use of pagers, text messaging, Internet, cell phones, etc.
  - The use of electronic devices allows them to dynamically respond to law enforcement action
  - Monitoring airwaves for intelligence

The Emerging Threats II

- Sleeper Agents
  - Already in place and waiting for attack?
  - Cyber and Human?
  - Don’t dismiss the potential for “insider placement” to meet a specific objective
- Lawyers
  - Legal liability associated with the lack of a diligent defense could have a significant impact on infrastructure operation
  - Department of Interior shutdown

The Emerging Threats III

- Organized Crime
  - Crime syndicates and gangs acting as domestic “mercenaries” for terrorist organizations
  - Could use disparate groups in a coordinated manner for sustained attacks
  - Proxy for physical attacks or institutional knowledge/human system attacks (e.g. assassination)
- Nation States
  - Mask action as originating from terrorists or rogue nations to achieve objective without attribution

Migrating Towards New Technologies

- Aum Shinryko cult developed software for over 80 Japanese firms and 10 agencies and was accessing law enforcement data
- Islamic Hacker Networks being formed
- Numerous low-level attacks against public information systems (e.g. Internet Black Tigers)
- Propaganda web sites increasing
- Private chat rooms, message boards, mailing lists
- Developing attack tools (virus, DOS)

The Threat Spectrum

- **Those with the intent, lack the capability**
  - Protective membrane of technology is quickly evaporating (COTS attack capabilities, MafiaBoy)
  - Long-term planning cycle could already be in effect
- **Those with the capability, lack the intent**
  - Economic interdependence, global condemnation, fear of conventional response create deterrence factor
  - "Unrestricted" type attacks become attractive if they can be launched anonymously or if framing can be conducted to divert response to a third party (e.g. bin Laden)

Why Information Terrorism?

- Continued focus within national security apparatus
  - PCCIP, PDD63, CIAO, NIPC, InfraGard, FIDNet, MOONLIGHT MAZE, SOLAR SUNRISE, ELIGIBLE RECEIVER!
  - Outsider perspective - “something significant here”
- Significant capability to disrupt the lives of citizenry
  - Attack launched from distributed environment - not geographically centralized. (targets too!)
  - Fits current terrorist mode of operation (asymmetrical cells)
  - Natural migration when physical resources are constrained

Why Information Terrorism? (II)

- Bytes not blood
  - Shock value of IW attack would not be as significant as a traditional terrorist attack, but the actual impact could be greater from a political perspective.
- Nearly impossible for military response to IW attack
  - "We reserve the right to respond in any way appropriate: through covert action, through military action, any one of the tools available to the president," Richard Clarke said at a Senate Judiciary subcommittee hearing on cyberterrorism.
  - Where do you send the tomahawks?
  - How do you determine who is responsible?
  - Are you every completely sure you've got the right perp (think unrestricted warfare)!

Asymmetrical Networks

…. The information revolution favors and strengthens network forms of organizations, while making life difficult for hierarchical forms…. It means conflict will increasingly be waged by "networks," rather than by "hierarchies". It means that whoever masters the network form stands to gain major advantages in the new epoch...

- John Arquilla and David Ron,

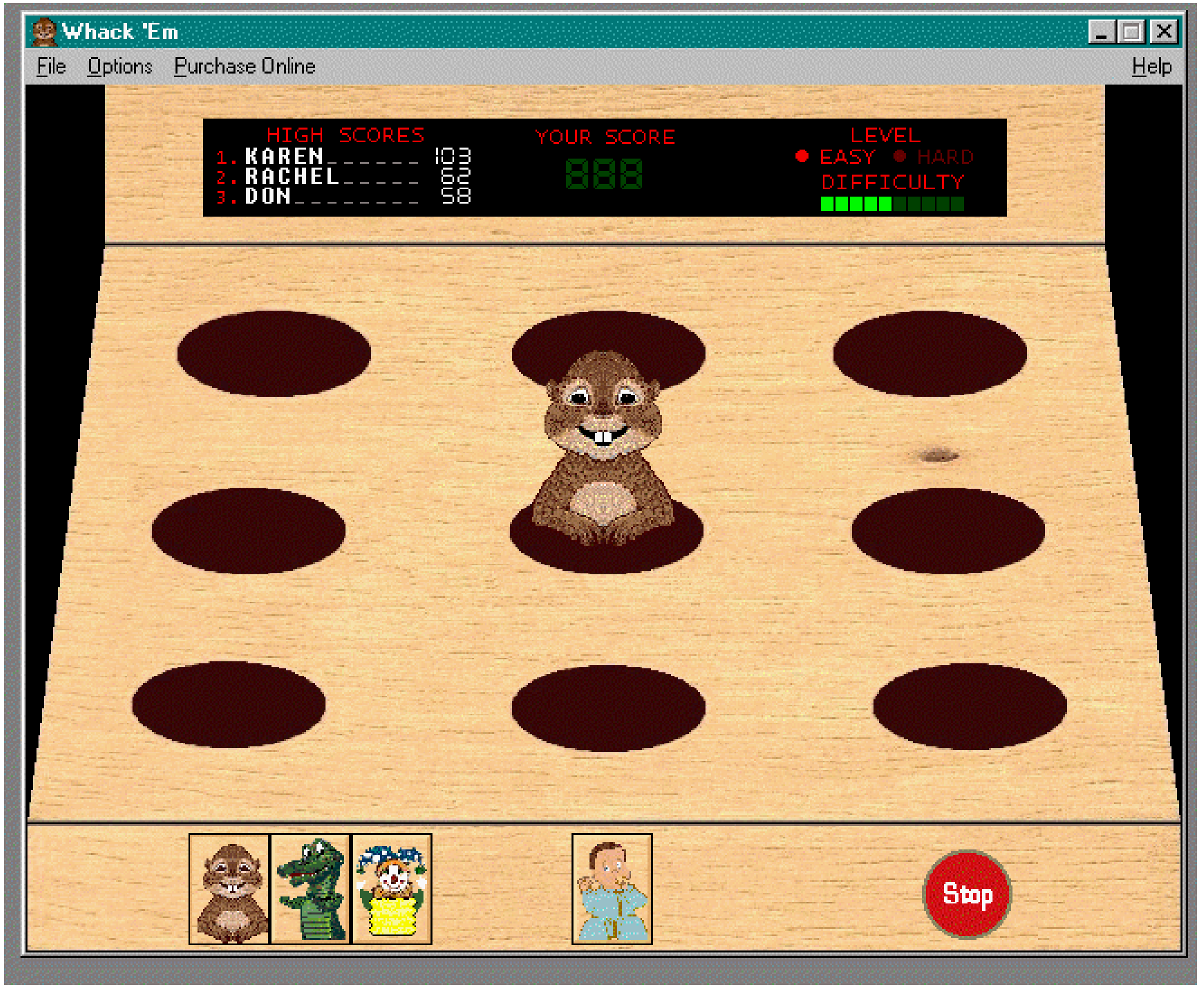
In Athena's Camp : Preparing for Conflict in the Information Age

Defending Against the Threat

Information Terrorism Toolkit?

Laptop with cellular phone, GPS unit, police scanner and misc. electronics.

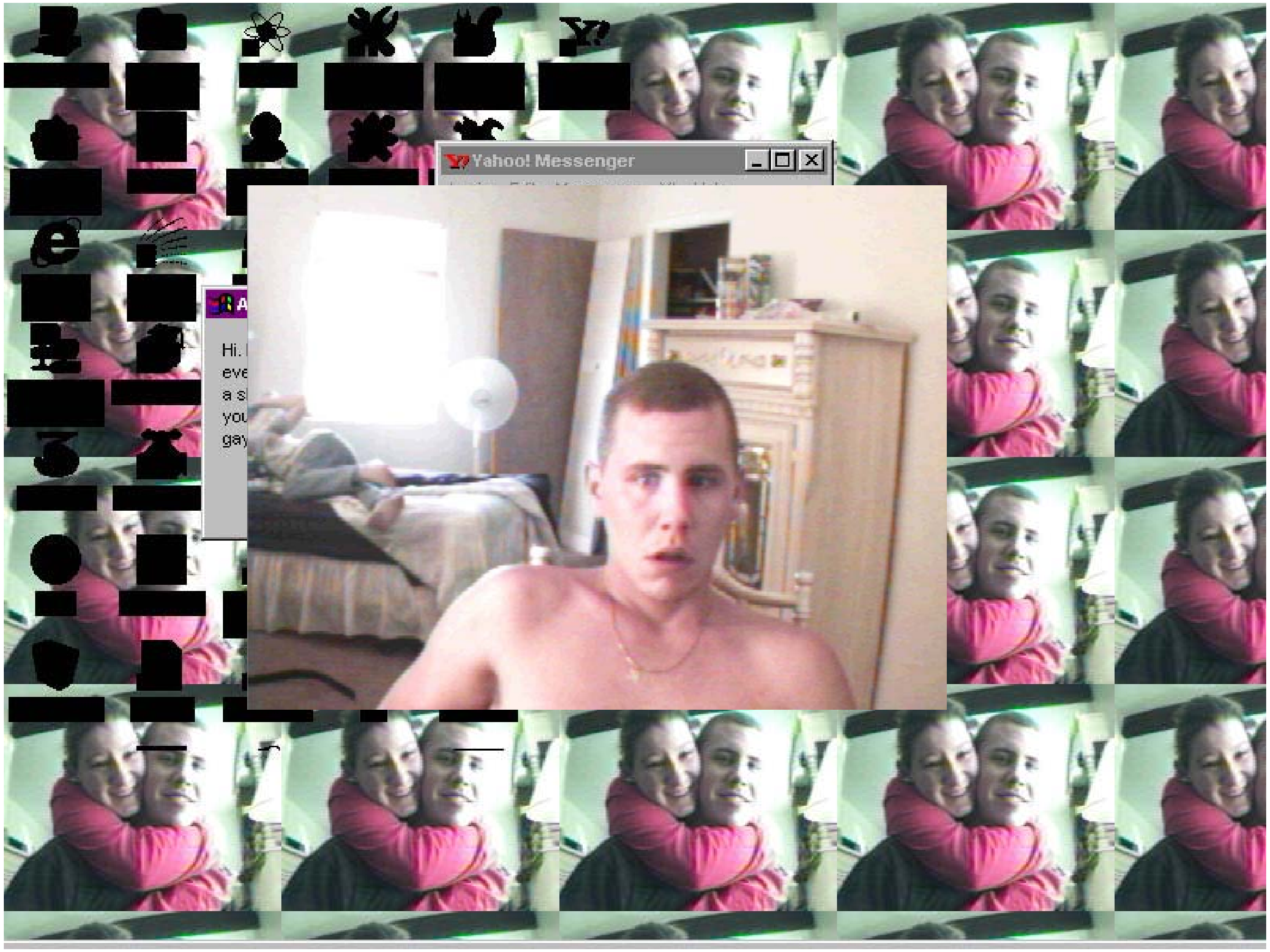
Current Response Model



HIGH SCORES

1.	KAREN	103
2.	RACHEL	62
3.	DON	58

It Could Happen to You!



[redacted]

Hi. I
eve
a s
you
gay

Threat Challenges

- Understanding the Threat
  - Real Attacks vs. False Alarms
    - Solar Sunrise, Moonlight Maze, or Red Dawn?
- Threat Analysis, Warning and Crisis Management Capability Needed!
  - PDD 63 calls for Information Sharing and Analysis Center (ISAC) – Where are we now?
  - Must facilitate information exchange between private and public sectors
  - Intrusion Detection and Network Monitoring capabilities need to be enhanced
  - Contextual threat assessments are required

Threat Challenges (II)

- Understand Our Vulnerabilities
  - Vigorous vulnerability analysis and red teaming required to understand our own weaknesses and secure potential targets
  - Oracle to Neo - “Know Thyself”
  - Requires significant expertise
  - Lesson of JWID CVAT - “Tools are not talent!”
- Security as a Design Concept
- Active Security Research Community

Searching for the Silver Bullet

- Scanning Tools
- Network Firewalls
- Intrusion Detection
- Virtual Private Networks (VPN)
- Encryption

Technology is not enough!

Avoid the "Silver Bullet" mentality when addressing technology deployment within your enterprise. Technology is not enough! Technology should only be deployed in support of a comprehensive security plan.

The Silver Concepts

- Diligent Defense
- Comprehensive Assessment
- Intelligence
- Response and Reconstitution

Diligent Defense

- Best practices help prevent the majority of attacks
- Policies and procedures are essential
- Formalized Risk Management process required (including valid threat models)
- Posture should reflect articulated information security policies
- I&W capability to determine when threat profile is changing

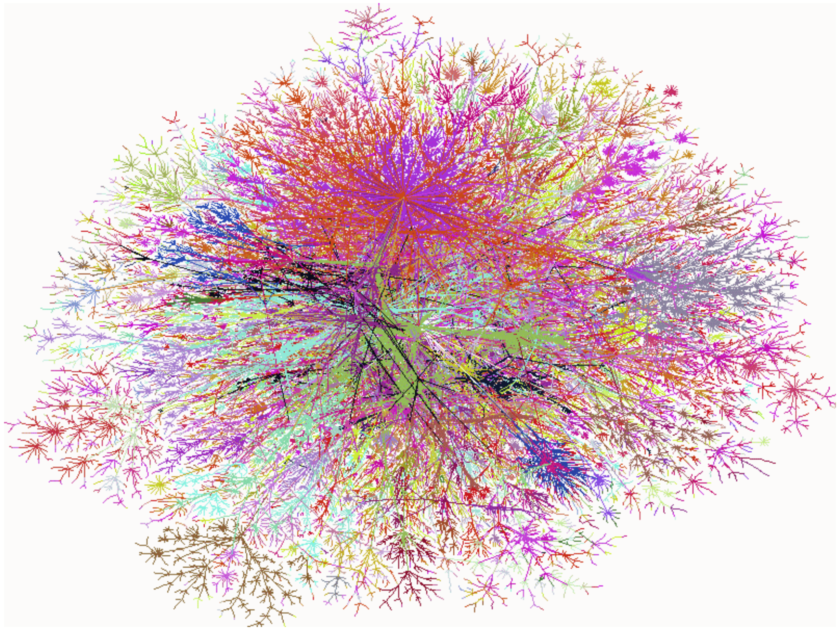
Assessment

- Strategic
  - An adversary can acquire a substantial capability without a significant investment, long-term development cycles, or readily observable testing or deployment
- Threat
  - Should be realistic
  - Feeds into Risk Management Process
- Self
  - Constant self assessment
  - Vulnerability assessments, certification and accreditation, red teaming – use the Experts!

The Power of Intelligence?

"The only effective way of countering terrorism is with good intelligence."

– David Kimche, Deputy Head - Mossad



There is nothing new about this!

Recognize the validity of adapting old models for new threats.

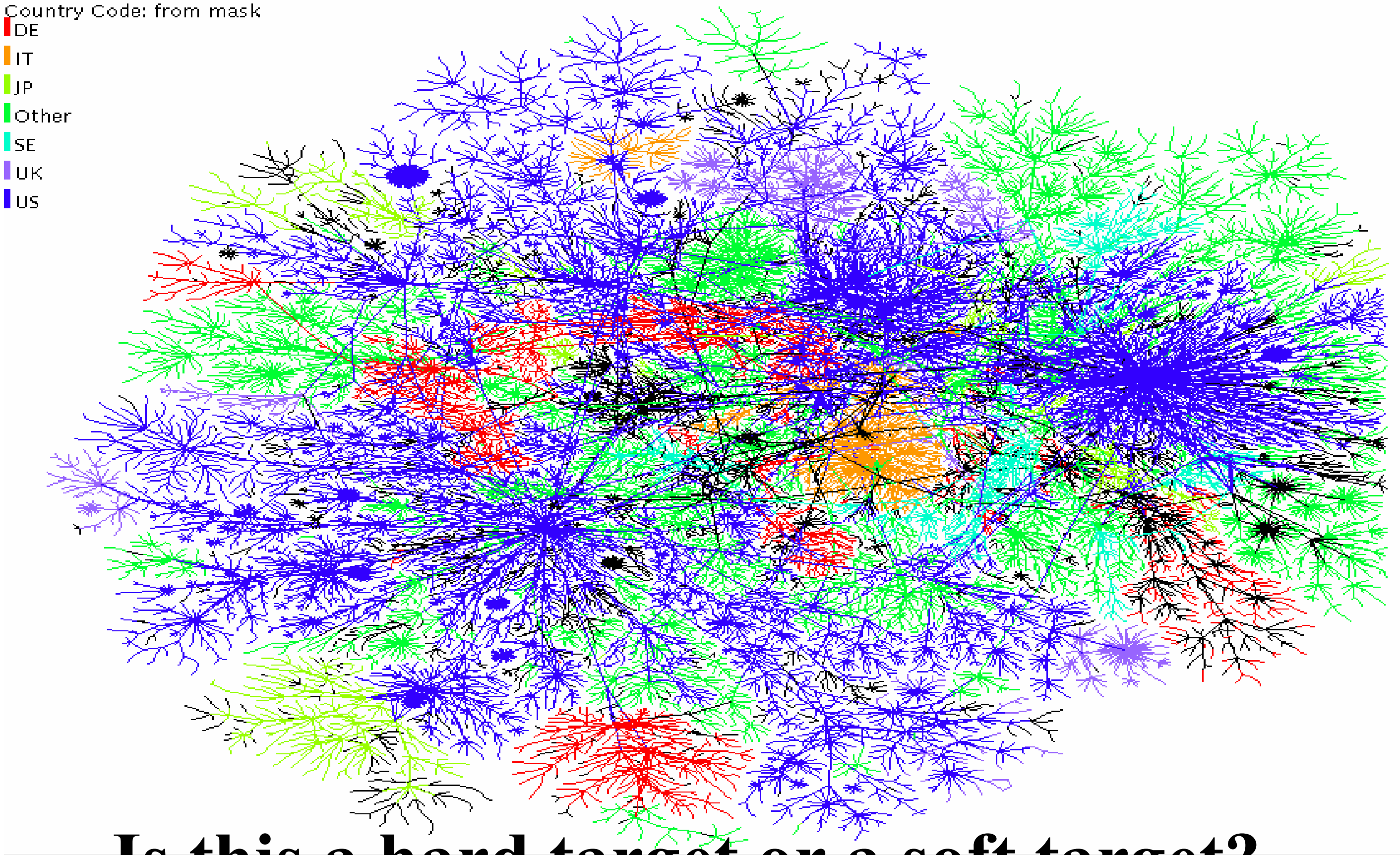
Intelligence

- ELIGIBLE RECEIVER had useful lessons, but so did SOLAR SUNRISE
  - *detection* of attack
  - source
  - strategy and scope of attack
- What about MOONLIGHT MAZE!?
- Accurate intelligence is only way to ensure proper response
- To maximize value, we must find mechanisms that allow for intelligence sharing (threat, vulnerability and incident information)

Response

- Plan and exercise your response capability
- All phases of the threat
  - Preemption
  - Active defense and attack containment
  - Damage control and mitigation
  - Reconstitution
  - Eliminate vulnerabilities as well as source of attack
- As with all other defensive mechanisms, this requires public/private cooperation, continuous assessment, and frequent and aggressive exercising.

Conclusion



Is this a hard target or a soft target?

Source: Internet Mapping Project – Bell Labs

For More Information

Terrorism Research Center – www.terrorism.com
Technical Defense, Inc. – www.technicaldefense.com

Matthew G. Devost
Devost@terrorism.com
Devost@technicaldefense.com
703-626-0272 (v)
703-832-8700 (f)